BASE4 SECURITY

ARG - MEX - CL - BRA - COL - PE - ESP - EEUU

POLÍTICA DE **SEGURIDAD DE LA INFORMACIÓN**

PRODIG.IO

Versión 01 - Marzo de 2024

Índice de contenidos

Política de Seguridad de la Información

INTRODUCCIÓN

Esta Política de Seguridad de la Información establece los principios y las directrices para proteger la confidencialidad, integridad y disponibilidad de los activos de información y garantizar la privacidad de los datos personales de las partes interesadas de **PRODIGIO**. Además, tiene como finalidad proporcionar un marco de referencia para establecer los objetivos de seguridad de la información, cumplir con la legislación aplicable, los requisitos vigentes de la norma ISO 27001 y promover la mejora continua.

ALCANCE

El presente documento se aplica en el marco del Sistema de Gestión de Seguridad de la Información, para todos las partes interesadas que tengan acceso o interactúen con activos de información de **PRODIGIO**.

OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

PRODIGIO tiene como propósito que su Política de Seguridad de la Información establezca las responsabilidades, directivas y requerimientos necesarios para garantizar la integridad, confidencialidad, trazabilidad y disponibilidad de la información. A tal fin, se deberá implementar una gestión del riesgo adecuada que permita aplicar controles de seguridad que permitan alcanzar un nivel tolerable de protección sobre los activos de información de la empresa.

Los principales objetivos de seguridad de la información son:

A. *Confidencialidad*: proteger la información contra accesos no autorizados o divulgaciones no permitidas, asegurando que solo las personas autorizadas puedan acceder a la información relevante para su desempeño laboral.

B. *Integridad*: garantizar que la información sea precisa, completa y esté actualizada, evitando modificaciones no autorizadas, pérdidas o destrucción indebida de los datos.

C. *Disponibilidad*: asegurar que la información esté disponible y sea accesible cuando sea requerida por los usuarios autorizados, minimizando las interrupciones no planificadas en los sistemas y servicios.

D. *Cumplimiento legal y regulatorio*: cumplir con todas las leyes, normas y disposiciones relacionadas a la seguridad de la información y la privacidad de los datos, incluida la protección de los datos personales.

E. *Responsabilidad*: incentivar a que las acciones y decisiones relacionadas con la seguridad de la información sean responsabilidad de todos los colaboradores.

RESPONSABILIDADES

A. *Alta Dirección*: establecer y mantener un marco de gobierno de seguridad de la información eficaz, adecuado y comprometido con la mejora continua.

B. *Comité de seguridad de la información:* evaluar y aprobar la implementación y actualización de los controles de seguridad y las evaluaciones de riesgo periódicas. Además, propiciar la capacitación y concientización en seguridad de la información a los colaboradores, a través de campañas y actividades de formación acorde a los roles y responsabilidades asignadas.

C. *Colaboradores y otras Partes Interesadas:* cumplir esta política, las normas y los controles de seguridad establecidos, proteger la información de la organización y reportar cualquier incidente de seguridad o brecha de datos, teniendo en cuenta el procedimiento implementado a tal fin.

D. *Gerencia de Ética y Compliance*: implementar y mantener el Sistema de Gestión de Seguridad de la Información, los controles de seguridad y de llevar a cabo evaluaciones de riesgos periódicas. Asimismo, incentivar a la capacitación y sensibilización sobre la seguridad de la información a los colaboradores a través de campañas y actividades formativas adecuadas a los roles y responsabilidades asignadas, entre otras tareas relacionadas, según las necesidades de la organización.

COMPROMISO DE LA DIRECCIÓN

La Alta Dirección de **PRODIGIO** se compromete a:

A. asegurar el establecimiento de la política y los objetivos de la seguridad de la información y su compatibilidad con la dirección estratégica de la organización;

B. garantizar la integración de los requisitos del SGSI con los procesos de la organización;

C. afianzar la disponibilidad de los recursos necesarios para el sistema de gestión de la seguridad de la información;

D. comunicar la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del SGSI;

E. asegurar que el SGSI logre los resultados previstos;

F. dirigir y apoyar a las personas, para contribuir a la eficacia del SGSI;

G. promover la mejora continua;

H. apoyar otros roles pertinentes de la dirección para que demuestren su liderazgo aplicado a sus áreas de responsabilidad.

DIVULGACIÓN Y COMUNICACIÓN

Esta Política de Seguridad de la Información deberá ser comunicada a todas las partes interesadas pertinentes. Del mismo modo, estará disponible y accesible para su consulta cuando fuera necesario.

CUMPLIMIENTO Y SANCIONES

Las partes interesadas se comprometen a cumplir con las disposiciones del presente documento y a contribuir a la seguridad de la información de PRODIGIO. Por otro lado, se los incentiva a reportar cualquier vulnerabilidad, amenaza o incidente de seguridad que detecten, garantizando un canal de comunicación seguro y, si es necesario, anónimo.

El incumplimiento de esta política puede dar lugar a acciones disciplinarias, teniendo en cuenta la gravedad de la situación, según corresponda.

REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada a intervalos planificados o si se produjeran cambios significativos en la estrategia u objetivos de la organización, a fin de garantizar su vigencia y eficacia.

Se realizarán evaluaciones de los objetivos y métricas de seguridad. Del mismo modo, se llevarán a cabo auditorías internas para verificar el cumplimiento de este documento. En consecuencia, se tomarán las acciones correctivas necesarias en caso de incumplimiento u oportunidad de mejora detectada.

TÉRMINOS Y DEFINICIONES

- **Alta Dirección:** se refiere a la persona o personas que gobiernan al más alto nivel una organización. Puede ser un director general, un gerente, un presidente, el consejo de administración, directores ejecutivos, socios directores, altos ejecutivos, etc.
- **Activos de Información:** cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.
- **Gestión de riesgo:** es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza a través de una secuencia de actividades humanas que incluyen la identificación, el análisis y la evaluación de riesgo, para luego establecer las estrategias de su tratamiento utilizando recursos gerenciales.
- **Partes interesadas:** persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad que sea relevante para el Sistema de Gestión de Seguridad de la Información.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** se refiere al diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la

confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información.

CONTROL DOCUMENTAL

Versión: **01** Vigencia: **14/03/2024** *Compliance Manager*	Revisión: **XX/XX/2024** *Comité de Seguridad de la Información*
Confidencialidad: **PÚBLICO**	

BASE4
SECURITY

www.base4sec.com